

UNITED STATES DISTRICT COURT  
for the  
District of New Mexico

FILED

United States District Court  
Albuquerque, New Mexico
  
Mitchell R. Elfers  
Clerk of Court

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

CHAVEZEDNA1107@GMAIL.COM AND  
JANIFERPENA5@GMAIL.COM THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE LLC

Case No. 21mr5

**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the NORTHERN District of CALIFORNIA, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 1028	Fraud and related activity in connection with identification documents
18 USC 1343	Fraud by wire, radio, or television

The application is based on these facts:

See Attached

- Continued on the attached sheet.
- Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Jessica Wright, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone \_\_\_\_\_ (specify reliable electronic means).

Date: Jan 4, 2021
  
Judge's signature

Laura Fashing, United States Magistrate Judge

Printed name and title

City and state: Albuquerque, NM

IN THE UNITED STATES DISTRICT COURT  
FOR NEW MEXICO

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
CHAVEZEDNA1107@GMAIL.COM AND  
JANIFERPENA5@GMAIL.COM THAT IS  
STORED AT PREMISES CONTROLLED  
BY GOOGLE LLC.

Case No. 21mr5

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Jessica Wright, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the U.S. Secret Service (“USSS”), and have been employed since December 2018. I am currently assigned to the USSS Albuquerque Resident Office, tasked to investigate violations of federal law relating to financial crimes and the

production, use and circulation of counterfeit United States currency. I have had formal training relating to these investigations during my 32-week Criminal Investigation Training Program at the Federal Law Enforcement Training Center in Glynco, GA and Special Agent Training Course in Beltsville, Maryland.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1028 (Fraud and related activity in connection with identification documents) and 18 U.S.C. § 1343 (Fraud by wire, radio, or television) have been committed by Janifer Baca. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

5. In relevant portion, 18 U.S.C. § 1028 provides as follows:

(a)(7) Whoever, in a circumstance described in subsection (c) of this section . . . knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law . . . shall be punished as provided in subsection (b) of this section.

\* \* \*

(b)(2)(B) The punishment for an offense under subsection (a) of this section is . . . except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more

than 5 years, or both, if the offense is . . . an offense under paragraph (3) or (7) of such subsection.

\* \* \*

(c)(3)(A) The circumstance referred to in subsection (a) of this section is that . . . the production, transfer, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means.

6. In relevant portion, 18 U.S.C. § 1343 provides as follows:

(a) Whoever . . . (1) having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means or wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing this scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

\* \* \*

### JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### PROBABLE CAUSE

8. On December 16, 2020, the United States Attorney’s Office in the District of New Mexico contacted the United States Secret Service (USSS) to request investigative assistance

regarding a voicemail from Edna Chavez with concerns of identity theft and social security fraud.

9. On December 18, 2020, Bernalillo County Sheriff's Office (BCSO) Detective Jordan Seay and USSS Special Agent Jessica Wright conducted an interview with Edna Chavez at her residence located at 24 Calle Manana, Belen, NM 87002. Ms. Chavez stated she is disabled; she suffers from osteoporosis and multiple sclerosis. Ms. Chavez obtained a caregiver, Janifer Baca (hereinafter "BACA"), through First Care of New Mexico LLC. BACA worked with Ms. Chavez from June 2019 – June 2020. Ms. Chavez fired BACA because she believes BACA fraudulently acquired approximately \$7,000 of her Supplemental Security Income (SSI).

10. Ms. Chavez stated starting in July 2020, BACA transferred one of her monthly SSI benefits for \$784.00, without permission or authorization, into a Direct Express debit card. Ms. Chavez believes BACA created and controls the Direct Express debit card. Several months ago, BACA accompanied Ms. Chavez to the Social Security Administration and helped Ms. Chavez set up the SSI monthly payment to be routed to a Direct Express debit card.

11. During this interview, Ms. Chavez provided numerous documents to include banking statements, deactivated Direct Express debit cards, and correspondence between the respective agencies authorized to provide payment to Ms. Chavez. Ms. Chavez's Wells Fargo bank statements show prior to July 2020, the \$784.00 SSI income payment was deposited into her account each month. Starting July 2020, the \$784.00 was no longer deposited into Ms. Chavez's Wells Fargo bank account.

12. Ms. Chavez explained that BACA accompanied her to the Social Security Administration and had her SSI monthly payment routed to a Direct Express debit card. A Direct Express card is a prepaid debit card offered to federal benefit recipients who receive their

benefits electronically. Direct Express headquarters is located in San Antonio, TX 78224. Ms. Chavez contacted Direct Express who advised that her \$784.00 SSI income is regularly deposited into a Direct Express debit card that is affiliated with CHAVEZ'S date of birth, social security number, address, however the name is under Edna Ortega. Direct Express would not discuss anything further regarding the account since the names were different.

13. Ms. Chavez stated that BACA fraudulently acquired approximately \$7,000 from her SSI benefits. Ms. Chavez explained that BACA was in her home four to five hours a day, seven days a week. BACA had access to all physical mail addressed to CHAVEZ, her cell phone, and email address. Ms. Chavez suspects that BACA used the information from an active Direct Express debit card and began transferring funds through a money transferring application via cell phone.

14. Ms. Chavez provided additional documentation that shows two associated Gmail accounts, [chavezedna1107@gmail.com](mailto:chavezedna1107@gmail.com) and [janiferpena5@gmail.com](mailto:janiferpena5@gmail.com) that can be managed from Ms. Chavez's cellphone. Ms. Chavez explained that one of those email addresses belongs to her and the other belongs to BACA. Ms. Chavez has never accessed BACA'S email account from her cellphone and does not know how it showed up on her cellphone.

15. Due to my training and experience, I know that debit and credit card transactions often occur in or affect interstate commerce. I also know that email and telephonic communications often make use of infrastructure located in states other than the state in which such communications originate. Furthermore, in my experience, opening bank accounts and credit card accounts typically requires the transfer of information in interstate commerce, whether by the mails or by telephonic or electronic means.

16. In general, an email that is sent to a Google LLC subscriber is stored in the subscriber's "mail box" on Google LLC servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google LLC servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google LLC's servers for a certain period of time.

**BACKGROUND CONCERNING EMAIL**

17. In my training and experience, I have learned Google LLC provides a variety of on-line services, including electronic mail ("email") access, to the public. Google LLC allows subscribers to obtain email accounts at the domain name gmail.com like the email account listed in Attachment A. Subscribers obtain accounts by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC subscribers) and information concerning subscribers and their use of Google LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

18. A Google LLC subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC . In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

19. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers, and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

20. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

21. In my training and experience, in some cases email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically

retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent

via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

### CONCLUSION

23. Based on the forgoing, I request that the Court issue the proposed search warrant.
24. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google LLC. Because the warrant will be served on Google LLC , who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

  
\_\_\_\_\_  
Jessica Wright  
Special Agent  
United States Secret Service

Subscribed, emailed electronically and sworn telephonically to before me  
on January 4, 2021:

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with Chavezedna1107@gmail.com and Janiferpena5@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on December, 31, 2020, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account from June 1, 2019 to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1028 and 18 U.S.C. § 1343, those violations involving BACA and occurring on or after June 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The contents of the electronic communications, subject to the limitations of the above paragraph, for Chavezedna1107@gmail.com and Janiferpena5@gmail.com, including attachments and stored files, stored or preserved copies of e-mails sent to and from the account, draft e-mails, deleted e-mails, e-mails maintained in trash or other folders, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail, and all existing printouts from original storage of the e-mails described above in Section I—

1. Tending to demonstrate the identity of the actual user(s) of the account;
2. Relating to identity theft or access device fraud, or to other violations of 18 U.S.C. § 1028 and 18 U.S.C. § 1343.
3. Containing account information for Chavezedna1107@gmail.com and Janiferpena5@gmail.com including:

- (i) Names and associated e-mail addresses;
- (ii) Physical address and location information;
- (iii) Records of session times and durations;
- (iv) Length of service (including start date) and types of service utilized;
- (v) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;
- (vi) The means and source of payment for such service (including any credit card or bank account number); and
- (vii) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service;
- (viii) All filter and forwarding settings.

4. User connection logs for Chavezedna1107@gmail.com and Janiferpena5@gmail.com for any connections to or from Chavezedna1107@gmail.com and Janiferpena5@gmail.com. User connection logs should include the following:

- (i) Connection time and date;
- (ii) Disconnect time and date;
- (iii) Method of connection to system (e.g., SLIP, PPP, Shell);
- (iv) Data transfer volume (e.g., bytes);

- (v) Internet Protocol addresses that were used when the user(s) connected to the service;
- (vi) Connection information for other systems to which user(s) connected via Chavezedna1107@gmail.com and Janiferpena5@gmail.com , including:
  - (1) Connection destination;
  - (2) Connection time and date;
  - (3) Disconnect time and date;
  - (4) Method of connection to system (e.g., telnet, ftp, http);
  - (5) Data transfer volume (e.g., bytes);
  - (6) Any other relevant routing information.
- (vii) Source or destination of any electronic communications sent from or received by Chavezedna1107@gmail.com and Janiferpena5@gmail.com , and the date, time, and length of the communications; and
- (viii) Any address to which electronic communications were or are to be forwarded from Chavezedna1107@gmail.com and Janiferpena5@gmail.com .

- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to 18 U.S.C. § 1028 (Fraud and related activity in connection with identification documents) and 18 U.S.C. § 1343 (Fraud by wire, radio, or television), including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC**  
**RECORDS PURSUANT TO FEDERAL RULES OF**  
**EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [PROVIDER], and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [PROVIDER]. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of [PROVIDER], and they were made by [PROVIDER] as a regular practice; and

b. such records were generated by [PROVIDER'S] electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of [PROVIDER] in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by [PROVIDER], and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature